REMARKS

With this Response, Applicants respectfully request that claims 1-21 be canceled without prejudice, and present new claims 22-41. Therefore, claims 22-41 are pending.

Objections to the Drawings

The Office Action states that new formal drawings will need to be submitted when the application is allowed. Please find that Applicants have filed new formal drawings herewith.

Claim Rejections - 35 U.S.C. § 101

Claims 1-9 were rejected under 35 U.S.C. § 101 as claiming non-statutory material. Specifically, claim 1 was rejected as claiming a non-functional, descriptive material, namely, a data string. Applicants have elected to cancel claims 1-9 herein; therefore, rejection of these claims is moot. New independent claims 22, 29, and 35 presented herein are directed to an apparatus, a method, and a stream cipher generator, respectively. Applicants respectfully submit that each of these is directed to functional elements, with claims 22 and 35 directed to physical "things," and claim 29 directed to "acts" to be performed. Thus, Applicants respectfully submit that each of these new independent claims is directed to statutory subject matter, and the dependent claims depending from these claims are also directed to statutory subject matter. Therefore, this rejection should not apply to the new claims presented herein.

Claim Rejections - 35 U.S.C. § 102

Claims 1-3, 7-13, and 17-21 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,703,952 issued to Taylor (*Taylor*). Applicants have elected to cancel these claims; therefore, rejection of these claims is moot. Applicants respectfully submit that the new

claims presented herein are not anticipated by the cited reference for at least the following reasons.

Claims 22-28

Claim 22 recites:

> a data bit generator to produce a principal data stream;
> multiple data bit generators to create additional data streams;
> a storage structure responsive to the additional data streams having multiple bit storage locations to **store the bits of the principal data stream in the storage locations in a pseudo random order based on an order of bits in the additional data streams**; and
> a shuffle unit coupled with the data bit generators to modify the principal data stream by combining the bits of the principal data stream with past bits of the principal data stream stored in the storage structure and pseudo randomly selected from the storage structure based on an order of the bits in the additional data streams to produce a pseudo random sequence.

Taylor discusses the use of a non-linear processor to provide non-linear feedback to combine with a message data stream (in the "integrity checking mechanism"). See Fig. 2; col. 10, line 61 to col. 11, line 14. *Taylor*'s non-linear feedback (also called the "memory data stream") is the output of a non-linear combination of its linear feedback shift registers (LFSRs). Regardless of whether *Taylor* calls its feedback "memory data," Applicants respectfully point out that the disclosure of *Taylor* is noticeably silent regarding storing data bits from a generated data stream in a storage structure, as recited in the claim. Even if *Taylor*'s feedback shift register were to be interpreted as a "storage structure" as claimed, which Applicants do not deny nor concede, Applicants point out that *Taylor*'s feedback shift register stores a non-linear combination of multiple generated data streams (col. 4, lines 2 to 15), and does **not** disclose storing bits of a generated principal data stream, as recited in the claim.

Even were *Taylor* to be so interpreted, which Applicants submit would be an improper interpretation of the reference, *Taylor* further fails to disclose or suggest that the bits are stored in

a pseudo random order, and much less that the pseudo random order may be based on an order of data bits in other data streams. Assuming for the sake of argument that *Taylor*'s shift register is a storage structure, *Taylor* is silent on any particular order in which bits are placed into the shift register, and what an order of the bits may be based upon. Thus, Applicants respectfully submit that *Taylor* fails to disclose either expressly or inherently every element of the claim, as required by MPEP § 2131 to establish a prima facie case of anticipation.

Claims 23-28 depend from claim 22. Because dependent claims necessarily include the limitations of the independent claims from which they depend, Applicants respectfully submit that these claims are not anticipated by the reference for at least the reasons set forth above with respect to the independent claim.

Claims 29-34

Claim 29 recites:

> generating a first and a second bit sequence;
> storing bits from the first sequence in a memory structure;
> **retrieving stored bits of the first sequence from the memory structure in a stochastic order, the order based at least in part on a bit order of the second sequence;**
> bit-wise modifying the bits of the first sequence with the stochastically retrieved bits to produce a pseudo random data stream.

As discussed above, *Taylor* discusses the use of non-linear feedback (called "memory bits") in producing a cipher stream, and fails to disclose or suggest the storing of bits of a generated data stream. Applicants further point out that *Taylor* fails to disclose or suggest that stored bits are retrieved from a memory structure in a stochastic order based on a bit order of a generated bit sequence, as recited in the claim. Assuming for the sake of argument that *Taylor* discloses storing bits of a generated data stream in a memory structure, Applicants note that *Taylor* is silent on any manner of storing to or retrieving bits from any such memory structure.

Therefore, Applicants respectfully submit that *Taylor* fails to disclose expressly or inherently every limitation of the claim as required by MPEP § 2131 to establish a prima facie case of anticipation.

Claims 30-34 depend from claim 29, and thus necessarily include the limitations of claim 29. Because it has been shown that the reference fails to anticipate independent claim 29, Applicants respectfully submit that it necessarily follows that the dependent claims are not anticipated for at least the same reasons set forth above for the independent claim.

Claims 35-41

Claim 35 recites:

> a first data bit generator to produce a first stream of data bits;
> a memory having a read and write port to receive and store bits from the first stream of data bits;
> a second data bit generator to produce a second stream of data bits;
> **a read and write port controller coupled to the memory and responsive to the second stream of data bits, to control the read and write functions of the memory based, at least in part, on the sequence of bits in the second stream of data bits**; and
> a combiner to receive the first stream of data bits and the bits read from the memory, and modify the first stream of data bits with the bits read from the memory to produce a pseudo random sequence.

For similar reasons as discussed above, *Taylor* fails to disclose or suggest storing bits from a generated stream of data bits in a memory. Furthermore, even assuming that *Taylor* could be so construed, which Applicants maintain would be a mischaracterization of the cited portions of the reference, Applicants respectfully submit that *Taylor*'s discussion of non-linear feedback fails to disclose or suggest controlling read and write functions of a memory based on the sequence of bits in a second stream of data bits, as claimed. Again, assuming for the sake of argument that *Taylor*'s feedback shift register is a memory, *Taylor* is silent on the manner in which reading and writing of bits is controlled to the shift register. Therefore, Applicants

respectfully submit that *Taylor* fails to disclose expressly or inherently every limitation of the claim as required by MPEP § 2131 to establish a prima facie case of anticipation.

Claims 36-41 depend from claim 35. Because dependent claims necessarily include the limitations of the independent claims from which they depend, Applicants respectfully submit that the reference fails to anticipate these claims for at least the same reasons set forth above with respect to the independent claims.

Claim Rejections - 35 U.S.C. § 103

Claims 4 and 14 were rejected under 35 U.S.C. § 103(a) as being "unpatentable over *Taylor* in lieu of obviousness." Claims 5-6 and 15-16 were rejected as being unpatentable over *Taylor* in view of U.S. Patent No. 6,069,954 issued to Moreau (*Moreau*). Applicants have elected to cancel these claims herein; therefore, rejection of these claims is moot. Applicants respectfully submit that these rejections do not apply to the new claims presented herein.

Assuming the rejection of claims 4 and 14 to be obviousness based upon the combination of *Taylor* and the understanding of one of skill in the art, Applicants note as far as Applicants can understand the rejection in the Office Action at page 8, it would appear that the Office Action cites *Taylor*'s use of the feedback shift register as "teaching toward" a storage structure having a plurality of addressable memory locations. Applicants are unable to understand the assertion/reasoning presented in the Office Action that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to place a memory unit at the output of first data bit generator and the input of the second data bit generator." To the extent that any of the new claims presented herein could be understood as including limitations similar to those of claims 4 and 14, which are herein canceled, Applicants would like to make clear that what the Office Action asserts is not what claims 4 and 14 recited. Rather, those claims recited "an input

port [of the memory] coupled to the first data bit generator, an output port, at least one read address port [also of the memory] and at least one write address port [also of the memory] coupled to the second data bit generator," which is in contrast to having a memory connected between two data bit generators, as asserted by the Office Action. Furthermore, even assuming that the assertion in the Office Action is correct, Applicants maintain that a rejection under *Taylor* of the new independent claims 22, 29, and 34 would be improper under MPEP § 2131, and the assertion made in the Office Action fails to cure the deficiencies of the reference discussed above.

Regarding *Moreau*, Applicants note that *Moreau* was cited as disclosing a de-multiplexer and a multiplexer. Whether or not *Moreau* discloses a multiplexer or a de-multiplexer, Applicants respectfully submit that *Moreau*'s discussion of a double XOR combining function and use of the Frogbit algorithm does **not** cure the deficiencies of *Taylor* discussed above. In summary, *Taylor* and *Moreau*, either alone or in combination, fail to disclose or suggest every element of the independent claims. Therefore, Applicants respectfully submit that a prima facie case of obviousness under MPEP § 2143 has not been established for the independent claims under the cited references. It necessarily follows that the dependent claims, which include all limitations of the claims from which they depend, are not rendered obvious by the references for at least the above reasons.

Conclusion

Applicants respectfully submit that all rejections have been overcome herein. Therefore, all pending claims are in condition for allowance, and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: 3/1/04

Gregory D. Caldwell
Reg. No. 39,926

12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
Telephone: (503) 684-6200

GDC/VHA

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on:

1 MARCH 2004
Date of Deposit

DEBORAH L. HIGHAM
Name of Person Mailing Correspondence

3/01/04
Signature **Date**